

09650323-032900

SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

BE IT KNOWN THAT WE, Hideki Akashika, a citizen of Japan residing at Koutou-ku, Tokyo-to, Japan, Shinichi Hirata, a citizen of Japan residing at Zushi-shi, Kanagawa-ken, Japan, Nagaaki Ohyama, a citizen of Japan residing at Kawasaki-shi, Kanagawa-ken, Japan and Akio Kokubu, a citizen of Japan residing at Minato-ku, Tokyo-to, Japan have invented certain new and useful improvements in

DATA STORING SYSTEM, ISSUING APPARATUS, DATA PROVIDING APPARATUS AND COMPUTER READABLE MEDIUM STORING DATA STORING PROGRAM

of which the following is a specification:-

EL594605483US

TITLE OF THE INVENTION

DATA STORING SYSTEM, ISSUING APPARATUS,
DATA PROVIDING APPARATUS AND COMPUTER READABLE
MEDIUM STORING DATA STORING PROGRAM

5

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a data
storing system, an apparatus and a computer readable
10 medium storing a data storing program. More
particularly, the present invention relates to a
data storing system, an apparatus and a computer
readable medium storing a data storing program for
storing data such as a program into an IC card and
15 the like by using a telecommunication system and the
like.

2. Description of the Related Art

Recently, a data storing system which uses
an apparatus having a high level of security such as
20 an IC card is becoming popular. An issuer (an IC
card issuer) stores an important data such as a
program in the apparatus when the issuer issues the
apparatus.

MULTOS is an example of a conventional
25 system wherein a system, called MULTOS-CA, which
guarantees data has authority to store a program to
a user apparatus (for example, an IC card) for
retaining security, and the issuer (IC card issuer)
in MULTOS stores the program in the user apparatus.
30 Therefor, there are problems that a data provider (a
service provider) which provides a program can not
let a user store the program which the data provider
provides, and that the data provider can not manage
information on storing a program.

35 In addition, there is no means for knowing
that a valid issuer and a valid data provider
acknowledges user's operation in which the user adds,

00650323 082900

changes, deletes data. Thus, there is a problem that data can not be stored in a user apparatus safely via network and the like.

Therefore, a data provider can store data only in a card which is issued by a specific IC card provider. That is, the data provider can not store data in a card which is issued by an IC card issuer which has no relation to the data provider. Therefore, it is needed that a data provider can store data safely into a card which is issued by any IC card issuer by performing certification with reliability.

SUMMARY OF THE INVENTION

It is an object of the present invention that the card issuer and the service provider equally can store and delete data in a card safely by mutual agreement between the user, the card issuer and the service provider.

Another object of the present invention is that each of the card issuer and the service provider can obtain information on data which is stored in an IC card.

Another object of the present invention is to register and manage the card issuer, the service provider and the user apparatus such that mutual certification can be performed. That is, the object is that the service provider can store data safely to a user apparatus and an issuer which are not any specific apparatus or issuer.

According to a first aspect of the present invention, the above object of the present invention is achieved by a data storing system comprising:

a user apparatus which stores data;
an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate;

00650323-082900

a data providing apparatus which is held
by a data provider that provides data;

an issuer registration apparatus which is
held by an issuer registrar that registers and
5 manages the issuer; and

a data registration apparatus which is
held by a data registrar that registers and manages
the data provider;

wherein the user apparatus comprises:
10 a registration information generation part
which generates registration information on a key
including a user public key or a part of a secret
key, sends the registration information to the
issuing apparatus with user information; and

15 a registration verification part which
verifies a registration certificate, received from
the issuing apparatus, which is signature
information or a hash value of the issuer for the
registration information and the user information,
20 stores the registration certificate to a storage
device when the registration certificate is
verified;

wherein the issuing apparatus comprises a
registration generation part which generates the
25 registration certificate and sends the registration
certificate to the user apparatus.

In the data storing system, the user
apparatus may further comprises:

a part which sends the registration
30 certificate and storing data information to the
issuing apparatus;

a part which verifies a storing
authorization when the storing authorization is
received from the issuing apparatus;

35 a part which verifies that the storing
data information corresponds to storing data which
is acquired; and

00650323 082900

a part which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data;

5 the issuing apparatus further comprising:
a part which verifies the registration certificate and the storing data information which are received from the user apparatus;

10 a part which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

15 a part which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus;

20 a part which verifies a storing authorization which is received from the data providing apparatus; and

a part which sends the storing authorization to the user apparatus when the storing authorization is verified;

25 the data providing apparatus further comprising:

a part which verifies the storing authorization request;

30 a part which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

35 According to a second aspect of the present invention, the above object of the present invention is achieved by an issuing apparatus in a

006280" E2E05950

5

15

20

25

35

key, sends the registration information to the issuing apparatus with user information; and

5 a registration verification part which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is
10 verified;

wherein the issuing apparatus comprises a registration generation part which generates the registration certificate and sends the registration certificate to the user apparatus,

15 the data providing apparatus comprising:

a part which receives the certificate registration, storing data information and a storing authorization request from the issuing apparatus;

20 a part which verifies the storing authorization request;

a part which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a
25 storing authorization, and sends the storing authorization to the issuing apparatus.

According to a fourth aspect of the present invention, the above object of the present invention is achieved by a computer readable medium
30 storing program code for causing a data storing system to store data, the data storing system comprising: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages
35 a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus

00650323 082900

5 computer readable medium comprising:

10 key, sends the registration information to the
issuing apparatus with user information; and

15 the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is

```
20    verified;
```

registration generation program code means, provided for the issuing apparatus, which generates the registration certificate and sends the registration certificate to the user apparatus.

25 The computer readable medium may further
comprises:

program code means, provided for the user apparatus, which sends the registration certificate and storing data information to the issuing

```
30 apparatus;
```

program code means, provided for the user apparatus, which verifies a storing authorization when the storing authorization is received from the issuing apparatus;

35 program code means, provided for the user
apparatus, which verifies that the storing data
information corresponds to storing data which is

acquired; and

program code means, provided for the user
apparatus, which stores the storing data into the
storage device when it is verified that the storing
5 data information corresponds to the storing data;

program code means, provided for the
issuing apparatus, which verifies the registration
certificate and the storing data information which
are received from the user apparatus;

10 program code means, provided for the
issuing apparatus, which provides certificate
information to the registration certificate and the
storing data information for generating a storing
authorization request when the registration
15 certificate and the storing data information are
verified; and

program code means, provided for the
issuing apparatus, which sends the registration
certificate, the storing data information and the
20 storing authorization request to the data providing
apparatus;

program code means, provided for the
issuing apparatus, which verifies a storing
authorization which is received from the data
25 providing apparatus; and

program code means, provided for the
issuing apparatus, which sends the storing
authorization to the user apparatus when the storing
authorization is verified;

30 program code means, provided for the data
providing apparatus, which verifies the storing
authorization request;

program code means, provided for the data
providing apparatus, which provides certificate
35 information to the storing authorization request and
the storing data information when the storing
authorization request is verified for generating a

0050323 082900

storing authorization, and sends the storing authorization to the issuing apparatus.

According to a fifth aspect of the present invention, the above object of the present invention
5 is achieved by a computer readable medium storing program code for causing an issuing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; the issuing apparatus which is held by
10 an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that
15 registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the computer readable medium comprising:

program code means which receives user
20 information and registration information on a key including a user public key or a part of a secret key from the user apparatus; and

registration generation program code means which generates registration certificate from the
25 registration information and the user information, and sends the registration certificate to the user apparatus.

According to a sixth aspect of the present invention, the above object of the present invention
30 is achieved by a computer readable medium storing program code for causing a data providing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; an issuing apparatus which is
35 held by an issuer that provides the user apparatus, and issues and manages a registration certificate; the data providing apparatus which is held by a data

00650323 082900

5

10

15

20

25

25

30

35

As mentioned above, in the present

invention, the user apparatus generates the registration information, sends it to the issuing apparatus with user information. The issuing apparatus stores the received registration
5 information and the user information, provides certificate information to the registration information, generates registration certificate, sends it to the user apparatus. The user apparatus verifies the received registration certificate,
10 stores it in a storage device if it is verified, such that data in an IC card can be stored and deleted safely.

According to the above-mentioned invention, by using the registration certificate which is
15 issued by the registration issuer, the party which receives the registration is insured. In addition, both of the card issuer and the service provider can perform processes such as data storing and data deleting safely.

20 In addition, the issuing apparatus, the data providing apparatus and the user apparatus verifies the registration certificate, the storing authorization request and the storing authorization such that tampering by a third party is prevented.

25 Further, each of the card issuer and the service provider can obtain information on data which is stored an IC card.

BRIEF DESCRIPTION OF THE DRAWINGS

30 Other objects, features and advantages of the present invention will become more apparent from the following detailed description when read in conjunction with the accompanying drawings, in which:

35 Fig.1 is a figure showing the principle of the present invention;

Fig.2 is a block diagram of a data storing

00650323 082900

system of the present invention;

Fig.3 is a diagram for explaining a general outline of the operation of the data storing system;

5 Fig.4 shows a system configuration for user registration according to a first embodiment of the present invention;

Fig.5 is a diagram for explaining a general outline of the operation of the data storing system when data is stored via an issuer according to a second embodiment;

Fig.6 is a block diagram of the data storing system when data is stored via the issuer according to the second embodiment;

15 Fig.7 is a diagram for explaining a general outline of the operation of the data storing system when data is stored via an data provider according to a third embodiment;

Fig.8 is a block diagram of the data storing system when data is stored via the data provider according to the third embodiment;

Fig.9 is a diagram for explaining a general outline of the operation of the data storing system when data is stored only by the data provider according to a fourth embodiment;

Fig.10 is a block diagram of the data storing system when data is stored only by the data provider according to the fourth embodiment;

Fig.11 is a diagram for explaining a general outline of the operation of the data storing system when a user apparatus is registered according to a fifth embodiment;

Fig.12 is a block diagram of the data storing system when a user apparatus is registered according to the fifth embodiment;

Fig.13 is a diagram for explaining a general outline of the operation of the data storing

00650323-082900

Fig.14 is a block diagram of the data storing system when data is stored according to the sixth embodiment;

Fig.16 is a block diagram of a computer
10 system which can be used as an issuing apparatus, a
data providing apparatus and the like.

Fig.1 and Fig.2 are figures of a data storing system for explaining the principle of the present invention. The data storing system includes a user apparatus 300 which stores data; an issuing apparatus 100 which is held by an issuer that provides the user apparatus 300, issues and manages a registration certificate; a data providing apparatus 200 which is held by a data provider that provides data; an issuer registration apparatus 400 which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus 500 which is held by a data registrar that registers and manages the data provider.

In the above-mentioned configuration, the user apparatus includes a registration information generation part 320 which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus 100 with user information; and a registration verification part 330 which verifies a registration certificate which is received from the issuing apparatus and which is signature information or a hash value of the issuer for the registration information and the user

5 The issuing apparatus 100 includes a registration generation part 120 which generates the registration certificate and sends the registration certificate to the user apparatus.

As mentioned above, as shown in Fig.2, the data storing system of the present invention includes an issuing apparatus 100, a data providing apparatus 200, a user apparatus 300, an issuer registration apparatus 400 and a data registration apparatus 500. The issuing apparatus 100 is owned by an issuer which provides the user apparatus, issues and manages a registration certificate. The data providing apparatus 200 is owned by a data provider which provides data. The user apparatus 300 stores the registration certificate and the data. The issuer registration apparatus 400 is owned by an issuer registrar which insures validity of the registration certificate. The data registration apparatus 500 is owned by a data registrar which insures validity of data.

Data can be exchanged between these apparatuses, for example, via communication lines, the Internet and the like. A tamperproof apparatus 30 (an IC card and the like) can be used for these apparatuses.

The issuing apparatus 100, the data providing apparatus 200, the issuer registration apparatus 400 and the data registration apparatus 500 generate and retain key information (such as a public key, a private key, a shared key, a part of a secret key and the like) for generating and

verifying a certificate which uses symmetric key cryptography, public key cryptography, digital signature method, secure hash method (message digest) or the like (which can be refereed in
5 "CONTEMPORARY ENCRYPTION THEORY", Ikeno, Koyama, IEICE.

In the following, a general outline of the operation of an embodiment of the present invention will be described with reference to Fig.3. Each of
10 the issuer registration apparatus and the data registration apparatus issues a registration certificate for the issuing apparatus and the data providing apparatus respectively by using a signature or the like. According to the
15 registration certificate, each of the issuing apparatus and the data providing apparatus can be proved to be valid.

The issuing apparatus issues a registration certificate to the user apparatus. An
20 application can be downloaded into the user apparatus via the issuing apparatus or via the data providing apparatus. An authorization for storing data is exchanged between the issuing apparatus and the data providing apparatus.

25 In the following, embodiments of the present invention will be described with reference to figures.

(first embodiment)

A first embodiment will be described with
30 reference to Fig.4. In this embodiment, the process of user registration between the user apparatus 300 and the issuing apparatus 100 will be described.

Fig.4 shows a system configuration for user registration of the first embodiment. This
35 system includes the issuing apparatus 100 and the user apparatus 300. The issuing apparatus 100 includes a database 110 and a certificate generation

00650323.082900

30 The certificate verification part 330
verifies validity of the registration certificate
(RC) input from the issuing apparatus 100. The
certificate verification part 330 verifies the
digital signature (or encrypted data, or secure
35 hash) of the registration certificate (RC). When
the registration certificate is valid, the
certificate verification part 330 stores the

registration certificate (RC) into the memory 310.

The operation of user registration is as follows.

(Step 11) The registration information generation part 320 in the user apparatus 300 generates the registration information for the issuing apparatus 100, stores the registration information (RI) into the memory 310, and sends the registration information (RI) to the issuing apparatus 100. When the issuing apparatus issues the registration information, this step 11 is not performed.

(Step 12) The certificate generation part 120 in the issuing apparatus 100 generates a registration certificate (RC) from the registration information (RI), stores it in the database 110, and sends it to the user apparatus 300.

(Step 13) The certificate verification part 330 in the user apparatus 300 verifies the registration certificate (RC), and stores the registration certificate (RC) in the memory 310 if it is verified.

(Second embodiment)

In this embodiment, the process of storing data (downloading of application) via the issuer will be described. First, the general outline will be described with reference to Fig.5.

In this process, the data registration apparatus 500 issues a data provider registration certificate to a data providing apparatus 200 in advance. (the processes (1) and (2) in Fig.5.

When the user apparatus 300 requests application download to the issuing apparatus 100 in step 21, the issuing apparatus 100 sends a storing authorization request to the data providing apparatus 200 in step 22. The data providing apparatus 200 issues a storing authorization to the

00650323-082900

Next, the second embodiment will be described in detail with reference to Fig.6. Fig.6 is a block diagram of the data storing system for data storing via the issuer according to the second embodiment.

The issuing apparatus 100 includes a certificate generation part 120, a certificate verification part 130 and a storing data
15 verification part 140.

The certificate generation part 120
35 receives verified a registration certificate (RC)
from the certificate verification part 130 and
receives verified storing data information (SDI)

from the storing data verification part 140. Then, the certificate generation part 120 generates a digital signature (or encrypted data, or secure hash) for the registration certificate and the storing data information, and sends the digital signature as a storing authorization request (SAR) to the data providing apparatus 200.

The data providing apparatus 200 includes a database 210, a certificate generation part 220, a certificate verification part 230 and a storing data verification part 240.

When the certificate verification part 230 acquires the storing authorization request (SAR) from the issuing apparatus, the certificate verification part 230 verifies the storing authorization request. When it is verified, the certificate verification part 230 sends the storing data information (SDI) to the storing data verification part 240 and sends the storing authorization request (SAR) to the certificate generation part 220.

The storing data verification part 240 writes the storing data information (SDI) which is received from the certificate verification part 230 into the database 210. In addition, the storing data verification part 240 verifies the storing data information (SDI). When it is verified, the storing data information (SDI) is sent to the certificate generation part 220.

The certificate generation part 220 verifies the storing authorization request (SAR) received from the certificate verification part 230 and verifies the storing data information (SDI) receives from the storing data verification part 240. When they are verified, storing authorization (SA) is sent to the issuing apparatus 100.

The user apparatus 300 includes a memory

00650323-082900

310, a certificate verification part 330 and a data verification part 340.

The certificate verification part 330 acquires the storing authorization (SA) from the
5 issuing apparatus 100, verifies it, and sends the verification result to the data verification part 340.

When the storing authorization (SA) is verified in the certificate verification part 330,
10 the data verification part 340 acquires storing data (APD) from the data providing apparatus 210, and writes the storing data (APD) into the memory 310.

In the following, the operation of the above-mentioned configuration in which data is
15 stored via the issuer will be described in detail.

(Step 21) The user apparatus 300 sends the registration certificate (RC) and the storing data information (SDI) to the issuing apparatus 100.

(Step 22) The issuing apparatus 100
20 verifies the registration certificate (RC) in the certificate verification part 130, and verifies the storing data information (SDI) in the storing data verification part 140. When both of them are verified, the issuing apparatus 100 generates the
25 storing authorization request (SAR) in the certificate generation part 120, and sends the registration certificate (RC), the storing data (SDI) and the storing authorization request (SAR) to the data providing apparatus 200.

30 (Step 23) The data providing apparatus 200 verifies the storing authorization request (SAR) in the certificate verification part 230, and verifies the storing data information (SDI). When both of them are verified, the data providing apparatus 200
35 generates a storing authorization (SA) for the storing authorization request (SAR) and the storing data information (SDI) in the certificate generation

006280" 082900 09650323

part 220, and sends the storing authorization (SA) to the issuing apparatus 100.

(Step 24) The issuing apparatus 100 verifies the storing authorization (SA) in the certificate verification part 130. When it is
5 verified, the issuing apparatus sends the storing authorization (SA) to the user apparatus 300.

Then, the user apparatus 300 verifies the storing authorization (SA) by using the certificate
10 verification part 330. The user apparatus 300 verifies that the storing data information (SDI) corresponds to storing data (APD) which is received in some way by using the data verification part 340. When it is verified, the storing data (APD) is
15 stored in the memory 310.

In the above-mentioned process, the user apparatus can delete the storing data (APD) which is already in the memory 310.

(third embodiment)

20 In the third embodiment, a case wherein data is stored via the data provider. The general outline will be described with reference to Fig.7.

In this embodiment, the data registration apparatus 500 issues a data provider registration
25 certificate to a data providing apparatus 200 in advance. (the processes (1) and (2) in Fig.7.)

When the user apparatus 300 requests application download to the data providing apparatus 200 in step 31, the data providing apparatus 200
30 sends a storing authorization request to the issuing apparatus 100 in step 32. The issuing apparatus 100 issues a storing authorization to the data providing apparatus 200 in step 33. Then, the data providing apparatus 200 downloads a requested application to
35 the user apparatus 100 in step 34.

Next, the third embodiment will be described in detail with reference to Fig.8. Fig.8

00650323-082900

is a block diagram of the data storing system for data storing via the data provider according to the third embodiment.

This system shown in Fig.8 includes a
5 issuing apparatus 100, a data providing apparatus 200 and a user apparatus 300.

The issuing apparatus 100 includes a certificate generation part 120, a certificate verification part 130 and a storing data
10 verification part 140.

When the certificate verification part 130 acquires the storing authorization request (SAR) from the data providing apparatus 200, the certificate verification part 130 verifies the
15 storing authorization request. When it is verified, the certificate verification part 130 sends the storing data information (SDI) to the storing data verification part 140 and sends the storing authorization request (SAR) to the certificate
20 generation part 120.

The storing data verification part 140 verifies the storing data information (SDI). When it is verified, the storing data information (SDI) is sent to the certificate generation part 120.

25 The certificate generation part 120 sends a digital signature (or encrypted data, or secure hash) as the storing authorization (SA) to the data proving apparatus 200. The digital signature proves that the storing authorization (SA) is generated by
30 the issuer on the basis of the storing authorization request (SAR) received from the certificate verification part 130 and the storing data information (SDI) received from the storing data verification part 140.

35 The data providing apparatus 200 includes a database 210, a certificate generation part 220, a certificate verification part 230 and a storing data

006280" 082900

verification part 240.

The certificate verification part 230 acquires the storing authorization (SA) from the issuing apparatus 100 and acquires a registration
5 certificate (RC) from the user apparatus 300, and verifies them.

The certificate generation part 220 receives the registration certificate (RC) from the certificate verification part 230 and receives the
10 storing data information (SDI) from the storing data verification part 240. Then, the certificate generation part 220 generates a storing authorization request (SAR) from them, and sends the storing authorization request (SAR) to the issuing
15 apparatus 100.

The storing data verification part 240 acquires storing data information (SDI) from the user apparatus 300. Then, the storing data
20 verification part 240 verifies the storing data information (SDI). When it is verified, the verification result (storing data information (SDI)) is sent to the certificate generation part 220.

The user apparatus 300 includes a memory 310, a certificate verification part 330 and a data
25 verification part 340.

The registration certificate (RC) is sent to the certificate verification part 230 of the data providing apparatus 200 from the memory 310, and the
30 storing data information (SDI) is sent to the storing data verification part 240 of the data providing apparatus 200.

The certificate verification part 330 acquires the storing authorization (SA) from the certificate verification part 230 in the data
35 providing apparatus 230, verifies the storing authorization (SA), and sends the verification result to the data verification part 340 when the

006280-2205960

storing authorization (SA) is verified.

The data verification part 340 acquires storing data (APD) from the database 210 in the data providing apparatus 200, and verifies the data.

- 5 When it is verified, the data verification part 340 stores the storing data (APD) into the memory 310.

In the following, the operation of the above-mentioned configuration in which data is stored via the provider will be described in detail.

- 10 (Step 31) The user apparatus 300 sends the registration certificate (RC) and the storing data information (SDI) to the data providing apparatus 200.

- 15 (Step 32) The data providing apparatus 200 verifies the registration certificate (RC) in the certificate verification part 230, and verifies the storing data information (SDI) in the storing data verification part 240. When both of them are verified, the data providing apparatus 200 generates
20 the storing authorization request (SAR) based on the registration certificate (RC) and the storing data (SDI) in the certificate generation part 220, and sends the registration certificate (RC), the storing data (SDI) and the storing authorization request
25 (SAR) to the issuing apparatus 200.

- (Step 33) The issuing apparatus 100 verifies the storing authorization request (SAR) in the certificate verification part 130, and verifies the storing data information (SDI) in the storing
30 data verification part 140. When both of them are verified, the issuing apparatus 100 generates a storing authorization (SA) for the storing authorization request (SAR) and the storing data information (SDI) in the certificate generation part
35 120, and sends the storing authorization (SA) to the data providing apparatus 100.

- (Step 34) The data providing apparatus 200

006280" 082900

verifies the storing authorization (SA) in the certificate verification part 230. When it is verified, the data providing apparatus 200 sends the storing authorization (SA) to the user apparatus 300.

5 Then, the user apparatus 300 verifies the storing authorization (SA) by using the certificate verification part 330. The user apparatus 300 verifies that the storing data information (SDI) corresponds to storing data (APD) which is received
10 in some way by using the data verification part 340. When it is verified, the storing data (APD) is stored in the memory 310.

 In the above-mentioned process, the user apparatus 300 can delete the storing data (APD)
15 which is already in the memory 310 instead of storing the storing data (APD).

(fourth embodiment)

 In this embodiment, data storing process only by the data provider will be described. The
20 general outline will be described with reference to Fig.9. In this embodiment, authorization by the card issuer may not be necessary for data download.

 In this embodiment, the data registration apparatus 500 issues a data provider registration
25 certificate to the data providing apparatus 200 in advance. (the processes (1) and (2) in Fig.9.)

 When the user apparatus 300 requests application download to the data providing apparatus
200 in step 41, the data providing apparatus 200
30 downloads a requested application to the user apparatus 300 in step 42.

 Next, the fourth embodiment will be described in detail with reference to Fig.10. Fig.10 is a block diagram of the data storing system
35 for data storing only by the data provider according to the fourth embodiment.

 This system shown in Fig.10 includes a

00650323-082900

data providing apparatus 200 and a user apparatus 300.

The data providing apparatus 200 includes a database 210, a certificate generation part 220, a
5 certificate verification part 230 and a storing data verification part 240.

The certificate verification part 230 acquires a registration certificate (RC) from the user apparatus 300, and verifies it.

10 The certificate generation part 220 verifies both of the registration certificate (RC) the storing data information (SDI). When they are verified, the certificate generation part 220 generates a storing authorization request (SAR) from
15 them, and sends the storing authorization request (SAR) to the user apparatus 300.

The user apparatus 300 includes a memory 310, a certificate verification part 330 and a data verification part 340.

20 The certificate verification part 330 acquires the storing authorization (SA) received from the data providing apparatus 200, and verifies the storing authorization (SA).

The data verification part 340 acquires
25 storing data (APD) from the data providing apparatus 200, and verifies the data. When it is verified, the data verification part 340 stores the storing data (APD) into the memory 310.

30 In the following, the operation of the above-mentioned configuration in which data is stored only by the data provider will be described in detail.

(Step 41) The user apparatus 300 sends the registration certificate (RC) and the storing data
35 information (SDI) to the data providing apparatus 200.

(Step 42) The data providing apparatus 200

00650323-082900

verifies the registration certificate (RC) in the certificate verification part 230. When it is verified, the data providing apparatus 200 generates the storing authorization (RC) based on the storing data information (SDI) in the certificate generation part 220, and sends the storing authorization (RC) to the user apparatus 300.

Then, the user apparatus 300 verifies the storing authorization (SA) by using the certificate verification part 330. The user apparatus 300 verifies that the storing data information (SDI) corresponds to storing data (APD) which is received in some way by using the data verification part 340. When it is verified, the storing data (APD) is stored in the memory 310.

In the above-mentioned process, the user apparatus 300 can delete the storing data (APD) which is already in the memory 310 instead of storing the storing data (APD).

(fifth embodiment)

Next, the fifth embodiment will be described. According to this embodiment, the registration process by the issuing apparatus will be described in detail. The general outline will be described with reference to Fig.11. In this embodiment, the issuer registration apparatus 400 issues an issuer registration certificate to the issuing apparatus 100 beforehand.

First, the user apparatus sends user information (a public key, a part of a secret key and the like) to the issuing apparatus 100 in step 51. Then, the issuing apparatus 100 generates a registration certificate based on the user information, and sends the registration certificate to the user apparatus in step 52.

The card issuer may generates a registration certificate from the user information

00650323 082900

and stores the registration certificate in a card which is provided to a user.

Next, the fifth embodiment will be described in detail with reference to Fig.12.

5 Fig.12 shows a block diagram of the data storing system at the time of user registration.

This system includes the issuing apparatus 100, the user apparatus 300 and the issuer registration apparatus 400.

10 The issuer registration apparatus 400 includes a database 410 and a certificate generation part 420.

The certificate generation part 420 acquires information (PKI) used for providing
15 certificate information from the issuing apparatus 100, generates an issuer registration certificate (IRC), stores it into the database 410, and sends it to the issuing apparatus 100.

The issuing apparatus 100 includes a
20 database 110, a certificate generation part 120, a certificate verification part 130 and a key information generation part 150.

The certificate generation part 120 generates a registration certificate (RC) from
25 registration information (RI) which is received from the user apparatus 300, stores the registration certificate (RC) into the database 110, and sends it to the user apparatus 300.

The certificate verification part 130
30 acquires the issuer registration certificate (IRC) from the issuer registration apparatus 400, and verifies the issuer registration certificate (IRC). When the issuer registration certificate (IRC) is verified, it is stored into the database 110.

35 The key information generation part 150 generates information (PKI) which is used for providing certificate information by the issuer.

00650323-082900

The issuing apparatus 300 includes a memory 310, a registration information generation part 320 and a certificate verification part 330.

5 The registration information generation part 320 generates registration information of information (RI) (a public key, a symmetric key in symmetric key cryptography, and the like) on a key such as a user public key or a part of a secret key and stores it in the memory 310.

10 The certificate verification part 330 acquires the issuer registration certificate (IRC) and the registration certificate (RC) from the issuing apparatus 100 and verifies them. When both of them are verified, they are stored in the memory
15 110.

In the above configuration, the issuing apparatus 100 may generate the registration information (RI) instead of receiving the registration information (RI) from the issuing
20 apparatus 100. In such a case, the issuing apparatus includes a registration information generation part.

Next, the operation of the above-mentioned configuration for user registration will be
25 described in detail.

(1) The issuing apparatus 100 generates information (key information) used for providing certificate information (used in the certificate generation part 120) by using the key information
30 generation part 150, and sends the information (PKI) (key information, or a part of the key information) to the issuer registration apparatus 400.

(2) The issuer registration apparatus 400 generates the issuer registration certificate (IRC)
35 by using the information (PKI) in the certificate generation part 420. Then, the issuer registration apparatus 400 stores the information (PKI) and the

00650323 082900

issuer registration certificate (IRC), and sends the issuer registration certificate (IRC) to the issuing apparatus 100.

5 The issuing apparatus 100 verifies the issuer registration certificate (IRC) in the certificate verification part 130. When it is verified, the issuer registration certificate (IRC) is stored in the database 110.

10 (Step 51) The user apparatus 300 generates registration information (RI) in the registration information generation part 320, stores it in the memory 310 and sends the registration information (RI) to the issuing apparatus 100. As mentioned above, the registration information (RI) can be
15 generated by the issuing apparatus.

(Step 52) The issuing apparatus 100 generates a registration certificate (RC) by using the received registration information (RI) in the certificate generation part 120, stores the
20 registration certificate in to the memory 110, and sends the registration certificate (RC) and the issuer registration certificate (IRC) to the user apparatus 300.

In addition, the user apparatus 300
25 verifies the registration certificate (RC) and the issuer registration certificate (IRC) by the certificate verification part 330. When both of them are verified, the registration certificate (RC) and the issuer registration certificate (IRC) is
30 stored in the memory 110.

(sixth embodiment)

In the following, the general outline of the sixth embodiment will be described with reference to Fig.13. In this embodiment, a
35 registration is issued to the data providing apparatus and a certificate is provided to application data.

006280 082900 09650323

As shown in Fig.13, the data registration apparatus 500 issues a registration to the data providing apparatus beforehand (the process shown in (1) and (2)).

5 When the user apparatus 300 sends storing data information to the data providing apparatus 200 in step 62, the data providing apparatus 200 issues a certificate of data in step 62. Then, the data providing apparatus 200 sends the data, the
10 certificate and the data provider registration certificate to the user apparatus in step 63.

Next, this embodiment will be described in detail with reference to Fig.14. Fig.14 shows a block diagram of the data storing system for data
15 storing according to the sixth embodiment.

This system shown in Fig.14 includes a data providing apparatus 200, the user apparatus 300 and the data registration apparatus 500.

20 The data registration apparatus 500 includes a database 510 and a certificate generation part 520.

 The certificate generation part 520 acquires information (PKD) for providing certificate information by the data provider from the data
25 providing apparatus 200, generates a data provider registration certificate (DPR) which is a digital signature of the data registrar to the information (PKD), stores the data provider registration certificate (DPR) in the database 510 and sends it
30 to the data providing apparatus 200.

 The data providing apparatus 200 includes a database 210, a certificate generation part 220, a certificate verification part 230 and a key information generation part 250.

35 The certificate generation part 220 acquires the storing data information (SDI) from the user apparatus 300 and storing data from the

00650323-082900

database 210. Then, the certificate generation part 220 generates storing data with a certificate (SDCI) which is the storing data (APD) and a digital signature to the storing data (APD) and the storing data information (SDI) which indicates data providing authorization. Then, the certificate generation part 220 sends the storing data (SDCI) with a certificate to the user apparatus 300.

The certificate verification part 230 acquires the data provider registration certificate (DPR) from the data registration apparatus 500 and verifies it.

The certificate verification part 330 acquires the data provider registration certificate (DPR) and the storing data with a certificate (SDCI) which is a digital signature of the data provider from the data providing apparatus 200. Then, the certificate verification part 330 verifies both of them. When they are verified, the certificate verification part 330 sends the storing data (APD) to the data verification part 340.

The data verification part 340 verifies the storing data (APD), and stored it into the memory 310 when it is verified.

The operation of the above-mentioned configuration will be described.

(1) The data registration apparatus 200 generates information (key information) used for providing certificate information (used in the certificate generation part 220) by using the key information generation part 250, and sends the information (PKD) (key information, or a part of the key information) to the data registration apparatus 500.

(2) The data registration apparatus 500 generates the data provider registration certificate (DPR) by using the information (PKD) in the

006280" 082900

certificate generation part 520. Then, the data registration apparatus 500 stores the information (PKD) and the data provider registration certificate (DPR) in the database 510, and sends and the data
5 provider registration certificate (DPR) to the data providing apparatus 200.

The data providing apparatus 200 verifies the data provider registration certificate (DPR) in the certificate verification part 230. When it is
10 verified, the data provider registration certificate (DPR) is stored in the database 210.

(Step 61) The user apparatus 300 sends the storing data information (SDI) on data to be stored to the data providing apparatus 200.

(Step 62, 63) The data providing apparatus
15 200 acquires necessary data information (APD) from the database 210 by using the received storing information. Then, the data providing apparatus 200 generates the storing data with a certificate (SDCI)
20 which is on the storing data information (SDI) and the storing data (APD) and sends the storing data with the certificate (SDCI) and the data provider registration certificate (DPR) to the user apparatus 300.

25 The user apparatus 300 verifies the storing data with the certificate (SDCI) and the data provider registration certificate (DPR) in the certificate verification part 330. When both of them are verified, the storing data (APD) which is
30 extracted from the storing data with the certificate (SDCI) is sent to the data verification part 340. Then, the data verification part 340 verifies that the storing data (APD) corresponds to the requested storing data information (SDI). When it is verified,
35 the storing data (APD) is stored in the memory 310.

(seventh embodiment)

In the above-mentioned sixth embodiment,

006280" 0205960

the data registration apparatus 500 may generate the storing data with the certificate (SDCI). In the following, the operation in this case will be described with reference to Fig.15 as a seventh embodiment. The configuration shown in Fig.15 does not includes the certificate generation part 220 and the key information generation part 250, instead, includes a storing data acquisition part 250.

First, the data providing apparatus 200 acquire the storing data (APD), which is stored by a user, from the database 210 by using the storing data information (SDI) as a key.

Next, the data providing apparatus 200 sends the storing data (APD) and information on the storing data (APD) (the storing data information (SDI), the size of the storing data (APD) or the like) to the data registration apparatus 500.

The data registration apparatus 500 generates a data certificate (SDCI') from the storing data (APD) and the information by using the certificate generation part 520, and stores the storing data (APD) and the data certificate (SDCI') in the database 510. Then, the data registration apparatus 500 sends the data certificate (SDCI') in the database 210.

The user apparatus 300 sends the storing data information (SDI), which is information on data to be stored, to the data providing apparatus 200.

The data providing apparatus 200 acquires data (SDCI) which includes the necessary storing data (APD), the data certificate (SDCI') and the information on the storing data (APD) from the database 210 by using the received storing data information (SDI), and sends the data (SDCI) to the user apparatus 300.

The user apparatus 300 verifies the data (SDCI) by using the certificate verification part

00650323 082900

330. When the data (SDCI) is verified, the storing
data extracted from the data (SDCI) is sent to the
data verification part 340. The verification part
340 verifies that requested data corresponds to the
5 extracted storing data (APD). When it is verified,
the storing data (APD) is stored in the memory 310.

The above-mentioned embodiments is
described on the basis of each element shown in each
figure. In addition, each element in the user
10 apparatus, the data providing apparatus, the data
registration apparatus, the issuing apparatus and
issuer registration apparatus can be constructed by
a program. The program can be stored in a disk
device which is connected to a computer which can be
15 used as the user apparatus, the data providing
apparatus, the data registration apparatus, the
issuing apparatus or the issuer registration
apparatus. In addition, the program can be stored
in a transportable recording medium such as a floppy
20 disk, CD-ROM and the like. By installing the
program stored in these medium to a computer, the
present invention can be realized.

The computer system which can be used the
issuing apparatus, the data providing apparatus and
25 the like may be configured as shown in Fig.15 for
example. The computer system includes a CPU 600
which executes processes, a memory 601 which stores
programs and data, a hard disk 602 which stores
programs and data used in the memory 601 or the CPU
30 600, a display 603 which displays data, a keyboard
604 for inputting data or commands and a
communication processing apparatus 605 which
performs communication with another computer via a
network. By installing a program which executes
35 processes of the issuing apparatus and the data
providing apparatus and the like which are described
in detail in each embodiment, the computer can be

006280" E2E05960

used as the issuing apparatus, the data providing apparatus and the like. The program is installed in the memory 601 or the hard disk 602, and executed by the CPU 600.

5 As mentioned above, according to the present invention, the following effects can be obtained.

(1) By the registration certificate which is issued by the registration issuer, the party
10 which receives the registration is insured. In addition, both of the card issuer and the service provider can perform processes such as data storing and data deleting safely.

That is, since the public key information
15 used for a certificate is certified by the registration issued by each registrar, the validity of the authorization is insured such that both of the card issuer and the service provider perform processes safely. In addition, since the issuer
20 which is certified issues the registration certificate of a card, the validity of the card is insured.

(2) By mutual agreement between the user, the card issuer and the service provider, the card
25 issuer and the service provider equally can store and delete data in a card safely.

That is, as mentioned above, since a party issues the storing authorization to another party which performs data download, data download is not
30 performed only by one of the card issuer and the service provider without authorization by another party such that data can be stored and deleted safely.

(3) Each of the card issuer and the
35 service provider can obtain information on data which is stored on an IC card.

That is, since data download is performed

005280" 22505960

after each of the user, the card issuer and the
service provider reaches an agreement, each of the
card issuer and the service provider can obtain
information on an application and a card which
5 stores the application.

In the future, as the number of
applications which are downloaded in IC cards
increases, it becomes important to obtain the above-
mentioned information.

10 In addition, according to the present
invention, a service provider can store data to a
card which is issued by any IC card issuer safely.

The present invention is not limited to
the specifically disclosed embodiments, and
15 variations and modifications may be made without
departing from the scope of the invention.

20

25

30

35

006280" E2E05950